Na pewno każdy interesujący się atakami w Sieci wie co to jest DoS i DDoS. Są to ataki polegające na przeciążeniu węzła w sieci. Takiemu węzłowi zaczyna brakować zasobów (mocy obliczeniowej, pamięci, łącza) i przestaje odpowiadać na zapytania.

Czy wiesz że jedna osoba i to z łączem na poziomie modemu jest w stanie położyć serwis internetowy, działający nawet na profesjonalnym serwerze?

Wszystko "dzięki" programowi Slowloris który wysyła zapytania HTTP ale... ich nie kończy. Zajmuje przez to zasoby serwera na obsługiwanie żądań, które czekają na więcej danych. W przypadku serwera Apache i kilku innych każde żądanie to osobny wątek, liczba wątków jest ograniczona a to powoduje "nasycenie" i niemożność przyjmowania nowych żądań dopóki działanie Slowlorisa nie zostanie przerwane.

Jak atakować?

Przede wszystkim jedynie własne serwery bo ataki DoS są karalne. Jednocześnie niniejszym zezwalam na atakowanie mojego serwera (a i tak to nie wyjdzie bo jest nginx, o tym później), o ile znasz mój adres IP.

Potrzebny będzie Perl (aptitude install perl) i kod "narzędzia". Piszemy w terminalu:

```
./slowloris -dns example.invalid
```

Pod example.invalid podstawiamy nazwę naszego celu. Ambitniejsi spojrzą do dokumentacji po opcje np. atakowania serwerów z SSL...

Serwer staje się z powrotem dostępny natychmiast po przerwaniu działania Slowlorisa - gniazda są zamykane i serwer ma miejsce na nowe wątki.

Jak się bronić?

Najprostszym sposobem jest zrezygnowanie z serwera Apache i zastąpienie go nginx (testowałem, polecam), lighttpd, Cherokee itd. Szczegóły na stronie Slowlorisa. Na atak podatny jest Apache i jakieś niepopularne serwerki, natomiast przed Slowlorisem dobrze bronią się "lekkie" serwery jak nginx oraz microsoftowy IIS.